

**DIGITAL ENCODING OF IMAGES OF SKIN-COVERED BODY PARTS****FIELD OF THE INVENTION**

The present invention relates generally to biometrics and, more particularly, to digital encoding of images of skin-covered body parts for use in a variety of applications.

**BACKGROUND**

Biometric recognition refers to the use of distinctive physiological (e.g., fingerprints, face, retina, iris) and behavioral (e.g., gait, signature) characteristics, called biometric identifiers (or simply biometrics) for automatically recognizing individuals. Because biometric identifiers cannot be easily misplaced, forged, or shared, they are considered more reliable for person recognition than traditional token- or knowledge-based methods. Specific applications where biometric identification is particularly useful include authentication and access control.

In the specific case of fingerprint recognition used for authentication of a person of interest, a management entity has knowledge of a target fingerprint image associated with the person of interest. When an individual who purports to be the person of interest provides a donor finger for scanning, the management entity compares the image of the donor finger with the target fingerprint image. In conventional automated fingerprint recognition, a search is done for matching features, or *minutiae*, in the two images. Examples of minutiae include core, delta, hook, ridge, bifurcation, island, lake, whorl, etc. For more information regarding fingerprint recognition in general, the reader is referred to D. Maltoni *et al.*, "Handbook of Fingerprint Recognition", Springer-Verlag, 2003, hereby incorporated by reference herein.

To accelerate both the transfer of the image of the donor finger to the management entity as well as the comparison process itself, the image may be encoded into a string of characters. Specifically, a feature extraction process is performed, whereby the minutiae are first located in the image and then the locations of the minutiae and their

1 type (ridge, island, etc.) are placed into an alphanumeric code. A similar code will  
2 have been previously generated by the management entity on the basis of the target  
3 fingerprint image. Thus, the authentication process consists of comparing the  
4 received code with the code stored at the management entity. A similar process  
5 occurs for access control to a facility, only the number of codes stored at the  
6 management entity may be far greater, since the identity of the purported donor is  
7 unknown *a priori*.

8  
9 While the aforementioned technique can work well in theory, there are practical  
10 considerations which compound and possibly even overshadow the technical  
11 difficulties associated with being able to accurately locate minutiae in a fingerprint  
12 image. Specifically, upon recognizing that the code produced from a fingerprint  
13 image encodes certain salient structural features (i.e., the minutiae), a malicious user  
14 having access solely to the alphanumeric code may be capable of partly reproducing  
15 the fingerprint image. This may violate certain privacy statutes relating to the  
16 communication or storage of an individual's personal information. Moreover, the  
17 problem does not dissipate by merely encrypting the code, since a sufficiently  
18 malicious user may be able to learn the necessary decryption method and hence gain  
19 knowledge of the minutiae.

20  
21 Clearly, therefore, a need exists in the industry for an improved technique to generate  
22 a code from an image of a skin-covered body part such as a finger, in such a way that  
23 reconstruction of minutiae or other salient structural features of the image will not be  
24 possible on the basis of the code alone.

## 25 26 27 SUMMARY OF THE INVENTION 28

29 According to a first broad aspect, the present invention seeks to provide a method of  
30 obtaining a digital code representative of a skin-covered body part. The method  
31 includes acquiring an image of the skin-covered body part, the image including a  
32 plurality of pixels, each pixel having an associated shade value in a range of shade  
33 values, followed by identifying a plurality of subsets of pixels from the plurality of  
34 pixels, each subset of pixels including at least two pixels having a common one of a

1 plurality of designated shade values in the range of shade values. Then, for each of a  
2 plurality of combinations of pixels taken from the pixels in the subsets of pixels, the  
3 method includes determining a geometric measure of the pixels in said combination.  
4 Finally, the method includes encoding the geometric measures into a digital code for  
5 the skin-covered body part.

6  
7 According to a second broad aspect, the present invention seeks to provide a  
8 computer-readable storage medium containing a program element for execution by a  
9 computing device to implement the above method of obtaining a digital code  
10 representative of a skin-covered body part, the program element including program  
11 code means for performing the various steps of the above method.

12  
13 According to a third broad aspect, the present invention seeks to provide an apparatus  
14 operative to control a state of an access point. The apparatus includes a biometric  
15 module adapted to acquire an image of a skin-covered body part submitted thereto and  
16 a processing module adapted for producing, responsive to acquisition of an image by  
17 the biometric module, a candidate code based on geometric measures of respective  
18 combinations of pixels taken from a plurality of subsets of like-shaded pixels in the  
19 image. The processing module is further adapted for causing a comparison to be  
20 performed between the candidate code and a set of references codes and, responsive  
21 to receipt of a signal indicative of the comparison yielding a match between the  
22 candidate code and one of the reference codes, sending a release signal to a restraint  
23 mechanism to cause the restraint mechanism to release the access point.

24  
25 According to a fourth broad aspect, the present invention seeks to provide a method of  
26 controlling a state of an access point. The method includes producing, responsive to  
27 acquisition of an image of a skin-covered body part submitted to a biometric module,  
28 a candidate code based on geometric measures of respective combinations of pixels  
29 taken from a plurality of subsets of like-shaded pixels in the image. The method  
30 further includes causing a comparison to be performed between the candidate code  
31 and a set of references codes and, responsive to receipt of a signal indicative of the  
32 comparison yielding a match between the candidate code and one of the reference  
33 codes, sending a release signal to a restraint mechanism to cause the restraint  
34 mechanism to release the access point.

1  
2 According to a fifth broad aspect, the present invention seeks to provide an apparatus  
3 that includes a communication interface capable of communication with a  
4 management entity over a network; a biometric module adapted to acquire an image  
5 of a skin-covered body part submitted thereto; an output device; and a processing unit.  
6 The processing unit is adapted for releasing a prompting signal via the output device,  
7 the prompting signal prompting submission of a skin-covered body part at the  
8 biometric module. Furthermore, responsive to acquisition of an image by the  
9 biometric module further to releasing the prompting signal, the processing module is  
10 adapted for producing a candidate code based on geometric measures of respective  
11 combinations of pixels taken from a plurality of subsets of like-shaded pixels in the  
12 image. Finally, the processing module is adapted for releasing the candidate code via  
13 the communication interface for comparison at the management entity with an  
14 expected code, thereby to verify presence of a person associated with the expected  
15 code.

16  
17 According to a sixth broad aspect, the present invention seeks to provide a method  
18 that includes releasing a prompting signal to prompt submission of a skin-covered  
19 body part at a biometric module. Furthermore, the method includes producing,  
20 responsive to acquisition of an image further to releasing the prompting signal, a  
21 candidate code based on geometric measures of respective combinations of pixels  
22 taken from a plurality of subsets of like-shaded pixels in the image. Finally, the  
23 method includes releasing the candidate code via the communication interface for  
24 comparison at the management entity with an expected code, thereby to verify  
25 presence of a person associated with the expected code.

26  
27 These and other aspects and features of the present invention will now become  
28 apparent to those of ordinary skill in the art upon review of the following description  
29 of specific embodiments of the invention in conjunction with the accompanying  
30 drawings.

31  
32  
33 **BRIEF DESCRIPTION OF THE DRAWINGS**  
34

1 In the accompanying drawings:

2

3 Fig. 1 is a block diagram of a biometric apparatus used for deriving a code from an  
4 acquired image of a skin-covered body part, in accordance with an embodiment of the  
5 present invention;

6

7 Figs. 2A-2D show plots of pixels at various stages of a process performed by the  
8 biometric apparatus in Fig. 1 to derive the code;

9

10 Fig. 3 is a flowchart showing steps in the process performed by the biometric  
11 apparatus in Fig. 1 to derive a code from the acquired image;

12

13 Fig. 4 shows a fingerprint image;

14

15 Fig. 5 shows a blown up portion of the fingerprint image of Fig. 4;

16

17 Figs. 6A and 6B are block diagrams of a system for controlling access through a door,  
18 in accordance with an embodiment of the present invention;

19

20 Fig. 7 is a flow diagram showing steps in a registration process executed at a  
21 management entity and at a door access module in the system of Figs. 6A and 6B, in  
22 accordance with an embodiment of the present invention;

23

24 Fig. 8 is a flow diagram showing steps in a monitoring process executed at the  
25 management entity and at the door access module in the system of Figs. 6A and 6B, in  
26 accordance with an embodiment of the present invention;

27

28 Fig. 9 is a block diagram of a system for electronic supervision of offenders, in  
29 accordance with an embodiment of the present invention; and

30

31 Fig. 10 is a flowchart showing steps in a supervision process executed at a  
32 management entity and a gathering process executed at a remote unit in the system of  
33 Fig. 9, in accordance with an embodiment of the present invention.

34



1 It is to be expressly understood that the description and drawings are only for the  
2 purpose of illustration of certain embodiments of the invention and are an aid for  
3 understanding. They are not intended to be a definition of the limits of the invention.  
4  
5

## 6 **DETAILED DESCRIPTION OF EMBODIMENTS**

7

8 As shown in Fig. 1, there is provided a biometric apparatus 12 for deriving a code 24  
9 from an acquired image of a skin-covered body part 18. In a specific non-limiting  
10 embodiment, the skin-covered body part 18 may be an individual's finger, whereas in  
11 other specific non-limiting embodiments, the skin-covered body part 18 may be an  
12 individual's ear, palm, forehead, nose, etc. Of course, the body part in its entirety is  
13 not required, and only a portion thereof may be used for the purposes of deriving the  
14 code 24.  
15

16 The biometric apparatus 12 includes a camera 14 and a source 16. The source 16  
17 emits light, which impinges on the skin-covered body part 18 pressed against a platen  
18 16A. A certain amount of the light impinging on the skin-covered body part 18 will  
19 be reflected/refracted towards the camera 14. In a specific non-limiting embodiment,  
20 the camera 14 may be a digital camera (e.g., a CMOS charge-coupled device), which  
21 produces a digital image 10 of the skin-covered body part 18. The biometric  
22 apparatus 12 also includes a computing device 20 equipped with a processor 20A, a  
23 memory 20B and an input/output interface (I/O) 20C. The computing device 20  
24 receives the digital image 10 from the camera 14 via the I/O 20C. The digital image  
25 10 is processed by the processor 20A in accordance with a process 22 (described later  
26 on in greater detail) to derive the aforementioned code 24 representative of the skin-  
27 covered body part 18.  
28

29 It should be understood that the present invention does not require the skin-covered  
30 body part 18 to be pressed against the platen 16A. Accordingly, the digital image 10  
31 may be acquired by a traditional camera setup that captures, from a distance, the  
32 ambient light reflected off of the skin-covered body part 18. In this way, the present  
33 invention may be applicable to the processing of facial images. In other embodiments  
34 contemplated by the present invention, the digital image 10 may be acquired at a

1 physically distinct location from the computing device 20 and transmitted thereto over  
2 a communication link and/or a network such as the Internet. In still other  
3 embodiments, the camera 14 may be a video camera that produces a video stream  
4 from which the digital image 10 can be derived.

5  
6 The functionality of the processor 20A may be implemented as pre-programmed  
7 hardware or firmware elements (e.g., application specific integrated circuits (ASICs),  
8 electrically erasable programmable read-only memories (EEPROMs), etc.), or other  
9 related components. In other embodiments, the processor 20A may be implemented  
10 as an arithmetic and logic unit (ALU) or a neural processor having access to a code  
11 memory (not shown) which stores program instructions for the operation of the ALU.  
12 The program instructions could be stored on a medium which is fixed, tangible and  
13 readable directly by the processor 20A, (e.g., removable diskette, CD-ROM, ROM,  
14 fixed disk, USB drive), or the program instructions could be stored remotely but  
15 transmittable to the processor 20A via a modem or other interface device.

16  
17 In accordance with a specific non-limiting embodiment of the present invention, and  
18 with additional reference to Figs. 4 and 5, the digital image 10 is comprised of an  
19 array of pixels 202. Each pixel 202 occupies a position in the digital image 10 and is  
20 associated with a shade value. The position of a given pixel 202 in the digital image  
21 10 can be defined by a point in a Cartesian plane with two orthogonal axes (denoted  
22 "X" and "Y") and an origin 204. The pixels 202 can thus be said to have "X" and  
23 "Y" coordinates. The number of pixels 202 in the array along each of the axes  
24 depends on operational requirements. For example, the number of pixels 202 along  
25 each axis may be the same or different.

26  
27 In the illustrated non-limiting example embodiment, the digital image 10 includes an  
28 array of 256 x 256 pixels 202, while the origin 204 for the purposes of positioning the  
29 pixels 202 is at the top left-hand corner of the digital image 10. In this case, the pixels  
30 202 will occupy coordinates ranging from (1,1) in the top left-hand corner (at the  
31 origin 204) to (256,256) in the bottom right-hand corner. It is envisaged that other,  
32 non-Cartesian, coordinate systems may be used for expressing the positions of the  
33 pixels 202. Also, the origin 204 could be placed at a different location, including in  
34 the center of the image or at the location of a salient feature of the image itself.

1  
2 As mentioned above, each of the pixels 202 is associated with a shade value. The  
3 range of possible shade values depends on operational requirements. For example, in  
4 one specific non-limiting example embodiment, the range of shade values for an 8-bit  
5 shade value may be from 0 to 255. In accordance with a specific non-limiting  
6 example embodiment of the present invention, the shade value of a pixel 202  
7 represents a level of gray of the pixel 202 and may be referred to as a gray scale value.  
8 For example, where 8-bit shade values are used, there are 256 resultant shades, which  
9 include absolute black, absolute white and 254 shades of gray in-between.

10  
11 In other specific non-limiting embodiments, a pixel 202 may initially be associated  
12 with a color triplet in a given color space, in which case the shade value of the pixel  
13 202 can represent the outcome of applying a color space processing function to the  
14 elements of the color triplet. Thus, for example, the pixel 202 may be associated with  
15 the color triplet  $(a, b, c)$  in the RGB color space or the YCbCr color space, while the  
16 shade value may be defined as, for example,  $\text{round}(\sqrt{a^2+b^2+c^2})$  or  
17  $\text{round}(\sqrt{a+b+c})$ . Naturally, the range of shade values will depend on the ranges of  
18  $a, b$  and  $c$ .

19  
20 As mentioned above, the processor 20A is adapted to execute the process 22 to derive  
21 the aforementioned code 24 representative of the skin-covered body part 18. With  
22 reference now to Fig. 3, as well as Figs. 2A through 2D, the process 22 is now  
23 described.

24  
25 Step 310

26  
27 The processor 20A selects a plurality of shade values from the range of shade values  
28 for further analysis. Specifically, if there are 256 possible shade values, then a certain  
29 number  $N \leq 256$  of the shade values will be selected and hereinafter referred to as  
30 “designated shade values”. The designated shade values may be known in advance by  
31 storing them in a database (not shown). The database itself may be stored in the  
32 memory 20B or may be accessible remotely through the I/O 20C. Alternatively,  
33 selection of the designated shade values may be performed based on a characteristic



of the image itself (such as whether the image is perceived to be that of a finger, ear, palm, etc.).

It should be understood that different values of  $N$  (i.e., different numbers of designated shade values) may lead to different levels of performance when measured in terms of the rate of false rejection, the rate of false acceptance and computational complexity. Also, depending on the quality and contrast of the digital image 10, the identity of the  $N$  designated shade values will also influence these parameters. Thus, it should be appreciated that different designated shade values may need to be used in different circumstances, and it is considered that the process of selecting the designated shade values is a task within the abilities of one skilled in the art.

### Step 312

The processor 20A identifies pixels having any of the designated shade values. This step, which can be viewed as performing a filtering operation on the digital image 10, results in a set of pixels that can be arranged to form a first table. The first table can be stored in the memory 20B. For example, the first table may be organized into rows, each row being associated with a given one of the designated shade values. The row associated with a particular designated shade value is either empty or contains either one or more pixels having the particular designated shade value. By saying that a row “contains a pixel” it should be understood that the row actually stores the coordinates of the pixel in question.

Consider the following example first table, whose pixels are plotted in Fig. 2A:

Designated shade value	Pixel(s)
15	<b>P</b>
63	<b>E, H</b>
77	
92	<b>Q</b>
112	<b>A, B, F, G</b>
186	
204	<b>C, D</b>
228	<b>R</b>
255	

**Example first table**

1

2 Step 314

3

4 Of course, it is possible that several neighboring or proximate pixels will each have a  
5 shade value that is one of the designated shade values. In this case, it may be  
6 advantageous to allow only one of these pixels to be entered into the designated shade  
7 table. In order to achieve this effect, and in accordance with optional step 314, it is  
8 within the scope of the present invention to prioritize the various designated shade  
9 values, such that in the event of two proximate pixels (say, within 8 or 10 pixels of  
10 one another) having different designated shade values, one of these shade values will  
11 take precedence and the corresponding pixel will be entered into the first table, while  
12 the other pixel will be ignored.

13

14 Similarly, it is within the scope of the present invention to prioritize different pixel  
15 positions, such that in the event of two proximate pixels having the same designated  
16 shade value, one of these pixels will take precedence based on its position (e.g.,  
17 relative to the origin 204 or a particular corner of the digital image 10), while the  
18 other pixel will not be entered into the first table. Various other methods for  
19 prioritizing nearby pixels will be apparent to those skilled in the art.

20

21 Consider the example first table, above, and the corresponding plot in Fig. 2A.  
22 Although not explicitly shown in Fig. 2A, it will be generally observed that a pixel-  
23 free border has been preserved around each pixel.

24

25 Step 316

26

27 The processor 20A removes all rows of the first table having fewer than two pixels.  
28 The result of step 316 may be the creation of a second table, which may be stored in  
29 the memory 20B. The rationale behind this elimination of empty or singleton rows is  
30 that useful geometric measures such as distance, area, etc. are not likely to be  
31 obtainable from a single pixel (or zero pixels, for that matter).

32

33 Consider the example first table, above. Application of step 316 results in the  
34 following example second table, whose pixels are plotted in Fig. 2B:

Designated shade value	Pixel(s)
63	<b>E, H</b>
112	<b>A, B, F, G</b>
204	<b>C, D</b>

**Example second table**Step 317

The processor 20A identifies a plurality of subsets of pixels from the various pixels in the second table created at step 316. Each subset of pixels so identified contains pixels sharing a common one of the designated shade values. The subsets can be identified in the following manner:

First Member of First Subset

To identify the first member of the first subset, the processor 20A may start at an initial search point (ISP) in the digital image 10. The first member of the first subset is identified as the pixel in any of the rows of the second table that is closest to the ISP. By way of example, the ISP may be the aforementioned origin 204 or it may be a different point in the digital image 10. Here, "closeness" may be defined relative to some measure of distance. By way of non-limiting example, the measure of distance between a pixel with coordinates  $(a,b)$  and a point with coordinates  $(c,d)$  can be the Euclidean distance  $\sqrt{(a-c)^2 + (b-d)^2}$ , or  $\min(|a-c|, |b-d|)$  or some other function of  $a$ ,  $b$ ,  $c$  and  $d$ .

Consider the example second table, above, and the corresponding plot in Figs. 2B and 2C. By locating the ISP towards the center of the drawing as in Fig. 2C, it will be seen that the closest pixel to the ISP is pixel **D**. This is the first member of the first subset.

Second Member of First Subset

Once the first member of the first subset has been identified, the processor 20A proceeds to identify the second member of the first subset. The second member of the first subset will be a like-shaded pixel, i.e., it will be in the same row of the second table as the first member of the first subset. Recalling that the rows of the second table each have at least two pixels, it will always be possible to find a second member of a given subset.

Specifically, where the row in question here has exactly two pixels, the second member of the first subset is the other pixel in the same row. Where the row in question here has more than two pixels, the second member of the first subset may be the next nearest like-shaded pixel, where “nearness” is defined relative to some measure of distance.

By way of non-limiting example, the measure of distance between one pixel with coordinates  $(a,b)$  and another pixel with coordinates  $(c,d)$  can be the Euclidean distance  $\sqrt{(a-c)^2 + (b-d)^2}$ , or  $\min(|a-c|, |b-d|)$  or some other function of  $a$ ,  $b$ ,  $c$  and  $d$ . One should keep in mind that alternative embodiments of the invention contemplate that the selection of the second member of a given subset may be based on criteria other than being the closest to the first member and, indeed, on criteria other than a distance altogether.

Consider the plot in Fig. 2C and the example second table, above. It will be seen that the only other pixel having the same shade value as pixel D is pixel C. This is the second member of the first subset.

#### Where Subsets Have Two Members

In accordance with one specific non-limiting embodiment, each subset is limited to containing a first member and a second member, even if some of the rows of the second table include more than two pixels. Therefore, after having found the first and second members of the first subset, step 317 proceeds with identifying the members of a second subset. Specifically, the first member of the second subset can be the pixel in the second table that is closest to the ISP, while of course ignoring those pixels that are already members of the first

subset. Next, the second member of the second subset will be a like-shaded pixel in the same row of the second table as the first member of the second subset. This process continues until a predetermined number say,  $M$ , of subsets have been identified, for a total of  $2 \cdot M$  pixels (since there are two members in each subset).

Consider again the plot in Fig. 2C and the example second table, above. It will be seen that three other two-member subsets can be formed using step 317, as indicated in the example third table, below. The pixels in the various subsets are plotted in Fig. 2C, with a link drawn between pixels in the same subset:

Subset	Pixel(s)
#1 (shade value 204)	<b>D, C</b>
#2 (shade value 112)	<b>F, B</b>
#3 (shade value 112)	<b>G, A</b>
#4 (shade value 63)	<b>E, H</b>

**Example Third Table**

Where Subsets Have More than Two Members

In accordance with another specific non-limiting embodiment, each subset consists of  $R$  members (a first member, a like-shaded second member and  $R-2$  like-shaded additional members), and therefore after having found the first and second members of the first subset, step 317 proceeds with identifying the  $R-2$  additional members of the first subset, using much the same technique as was used for identifying the second member of the first subset.

After having identified all the members of the first subset, step 317 proceeds with identifying a second subset, which begins with identifying a first member of the second subset. This can be the pixel in the second table that is nearest the ISP, while of course ignoring those pixels that are members of the first subset. The  $R-1$  other members of the second subset will be like-shaded pixels in the same row of the second table as the first member of the second subset, and so on. This process continues until a predetermined number say,  $M$ , of



subsets have been identified, for a total of  $R*M$  pixels (since there are  $R$  members in each subset).

It is noted in both of the above cases that each of the  $M$  identified subsets of pixels will contain pixels sharing a common one of the designated shade values.

#### Step 318

The processor 20A then makes a plurality of combinations of the pixels taken from the various pixels in the aforementioned third table. In the simplest case, each of the combinations of pixels corresponds to an individual one of the previously described subsets of pixels. In a slightly more complex case, each of the combinations of pixels includes members from more than one of the subsets of pixels. Of course, various other ways of mapping the subsets of pixels to combinations of pixels will be apparent to those of ordinary skill in the art, including mappings that result in the number of combinations being different from the number of subsets.

Consider the example third table, above. Assume also that each combination of pixels includes two pixels and, specifically, where the first pixel in the  $X^{\text{th}}$  combination is the first pixel in the  $X^{\text{th}}$  subset and where the second pixel in the  $X^{\text{th}}$  combination is the second pixel in the  $((X \text{ MOD } M)+1)^{\text{th}}$  subset. This results in the following example fourth table, whose pixels are plotted in Fig. 2D, with a link drawn between pixels in the same combination:

Combination	Pixel(s)
#1	D, B
#2	F, A
#3	G, H
#4	E, C

**Example Fourth Table**

It is noted that the pixels in a given combination do not necessarily have the same shade value.

#### Step 319

Once the combinations of pixels have been formed and put into the aforementioned fourth table, a geometric measure of the pixels in each combination is determined.

In the simplest case, where each combination of pixels includes only two members, the geometric measure of the two pixels in the combination of pixels may be a measure of distance between the two pixels. By way of non-limiting example, the measure of distance between one pixel with coordinates  $(a,b)$  and another pixel with coordinates  $(c,d)$  can be the Euclidean distance  $\sqrt{(a-c)^2 + (b-d)^2}$ , or  $\min(|a-c|, |b-d|)$  or some other predefined function of  $a$ ,  $b$ ,  $c$  and  $d$ . In another non-limiting embodiment, the measure of distance may be a couple  $(d_x, d_y)$  defined by  $(|a-c|, |b-d|)$ .

Consider the example fourth table, above, and the corresponding plot in Fig. 2D. The distances between the respective pairs of pixels in each of combinations #1, #2, #3 and #4 can be denoted  $\Delta 1$ ,  $\Delta 2$ ,  $\Delta 3$  and  $\Delta 4$ , respectively.

Where each subset of pixels includes more than two members (say,  $R$  members), the geometric measure of the  $R$  pixels in the combination of pixels may be the area (in square pixels or the like) of a polygon formed by interconnection of the  $R$  pixels; alternatively, the geometric measure could be the average distance between all possible pairs of pixels formed from the  $R$  pixels; alternatively, the geometric measure could be the average distance from each pixel to the center of mass of the  $R$  pixels; still other geometric measures will be apparent to those skilled in the art.

#### Step 320

The geometric measures obtained at step 319 are assembled into the code 24 representative of the skin-covered body part 18. This process may be as simple as concatenating the various geometric measures into a binary word, which can have a length on the order of several hundred bits or several kilobits (kb), depending on the number of combinations and on the number of bits used to encode each geometric measure. For example, consider the aforementioned distances  $\Delta 1$ ,  $\Delta 2$ ,  $\Delta 3$  and  $\Delta 4$ . These may be concatenated to give a code 

$\Delta 1$	$\Delta 2$	$\Delta 3$	$\Delta 4$
------------	------------	------------	------------

.

1  
2 In a variant, the designated shade values for the geometric measures may also form  
3 part of the code 24 and, in fact, an association between the geometric measures and  
4 the designated shade values may be built into the code 24.

5  
6 It is also within the scope of the present invention to enhance security by optionally  
7 encrypting the code 24. This can be done in a way that would be understood to a  
8 person skilled in the art, including using a public or private key or other cryptographic  
9 methods.

10  
11 It should be understood that some of the steps in Fig. 3 may be preceded or followed  
12 by additional image processing operations that alter the digital image 10 to enhance or  
13 suppress certain features. Non-limiting examples of additional image processing  
14 operations that may be used include thinning, erosion, opening, pruning, thickening,  
15 skeletonization, thresholding, etc.

16  
17 From the above, it will be apparent that the code 24 is derived in such a way that there  
18 is a very low probability that different skin-covered body parts will produce the same  
19 code 24. That is to say, the code 24 derived from an image of a given skin-covered  
20 body part will be unique to that body part. At the same time, it will be recognized that  
21 the code 24 in and of itself provides no information about the geometric  
22 characteristics of the digital image 10 (such as minutiae in the case of a fingerprint  
23 image). In fact, because the code 24 does not reveal information about pixel  
24 coordinates within the digital image 10, it would be extremely difficult, if not  
25 impossible, to meaningfully reconstruct the digital image 10 on the basis of the code  
26 24 alone.

27  
28 Hence, it will be appreciated that the approach presented herein is suitable for  
29 application in areas of endeavor where privacy concerns are a consideration.  
30 Examples of specific areas of application include access control and offender  
31 supervision, both of which will now be described in greater detail.

32  
33 Application #1: Access Control  
34

1 With reference now to Fig. 6A, there is shown a system for controlling access through  
2 an access point of a facility. In the specific non-limiting example embodiment that  
3 will be developed herein below, the access point is a door 602. However, it should be  
4 understood that the access point may be something other than a door, such as a  
5 turnstile, a window, a vault, a revolving door, an elevator, a gate and so on.

6  
7 In the specific case where the access point is the door 602, the system includes a door  
8 access module 604 and a management entity 606, which are connected to one another  
9 by a communication link 608. In some embodiments, the door access module 604  
10 may be individually installed for each door 602, whereas in other embodiments, the  
11 door access module 604 may control multiple doors, including door 602.  
12 Furthermore, in some embodiments, the door access module 604 may be installed on  
13 or in the door 602, whereas in other embodiments, the door access module 604 may  
14 be installed on or in the wall next to the door 602. In still other embodiments,  
15 especially where multiple doors are to be controlled at the same time from a remote  
16 location (e.g., in a prison), the door access module 604 may be installed in an area to  
17 which entry is not restricted using the door access module 604. Still other  
18 embodiments contemplate installation of the door access module 604 as a component  
19 of a wireless handheld device.

20  
21 In some embodiments, the management entity 606 may be located in a security room  
22 or the like. In other embodiments, the management entity 606 may be embodied as a  
23 component of a wireless handheld device. In still other embodiments, the  
24 management entity 606 may be located at premises that are connected to the door access  
25 module 604 over at least one network such as the Internet.

26  
27 Of course, the present invention is not limited to control of a single door and it should  
28 be understood that access to any number of doors could be controlled in an identical  
29 fashion as will be described for the door 602.

30  
31 The management entity 606 includes a biometric apparatus 610 (or “biometric  
32 module”), a memory 612, a communication interface 614, a processor 616 and a  
33 display 626 (or other output device). It should be understood that the words  
34 “processor” and “controller” are used in the following merely to distinguish between

1 functionality executed at a central location (by a processor) and functionality executed  
2 at a remote location (by a controller). Thus, one will appreciate that this has been  
3 done for the sole purpose of improving readability, and is not intended to limit the  
4 scope of either the term “processor” or “controller”. Rather, the two terms are to be  
5 interpreted broadly, as referring to entities capable of executing various processing  
6 and/or control functions.

7  
8 The biometric apparatus 610 is operable to produce a code 618 on the basis of an  
9 object submitted to it during a so-called “registration” process. In the expected  
10 scenario, the object submitted to the biometric apparatus 610 is a skin-covered body  
11 part 620 of a user 622 who is authorized to have some level of authorization to open  
12 the door 602. Thus, the code 618 will be representative of the skin-covered body part  
13 620 of the user 622. In accordance with an embodiment of the present invention, the  
14 code 618 is derived based on geometric measures of combinations of pixels taken  
15 from a plurality of subsets of like-shaded pixels in an image of the skin-covered body  
16 part 620. An example of a suitable technique for generation of the code 618 may be  
17 based on that described above with reference to Fig. 3.

18  
19 The memory 612 is used to store the code 618 along with other access control  
20 information 619 for the user 622, such as an identity of the user 622 (e.g., a user ID),  
21 access restrictions (e.g., time-of day and/or day-of-week), a history of previous  
22 accesses to the door 602, and so on. Similarly, the memory 612 stores other codes  
23 618A, 618B for other registered users in addition to respective access control  
24 information 619A, 619B similar to the preceding. Of course, where multiple doors  
25 exist, the access control information for various users may be stored on a per-door  
26 basis. However, and for the sole purpose of simplifying the description, it is assumed  
27 that there is only one door (i.e., the door 602).

28  
29 In order to reduce the risk of personal information being leaked or stolen from the  
30 memory 612, the code 618 output by the biometric apparatus 610 should not provide  
31 sufficient information to allow reconstruction of a meaningful image of the skin-  
32 covered body part 620 from which the code 618 was derived. To this end, the  
33 biometric apparatus 610 is preferably the biometric apparatus 12 described above with  
34 reference to Figs. 1-4, 5A and 5B.



1  
2 The communication interface 614 allows the management entity 606 to communicate  
3 with the door access module 604 over a communication link 608. In one specific non-  
4 limiting embodiment, the communication link 608 is a wireless link. One advantage  
5 of a wireless link is that cabling between the management entity 606 and the door  
6 access module 604 is not required, thus potentially lowering costs. In another specific  
7 non-limiting embodiment, the communication link 608 is a LAN (e.g., an Ethernet  
8 link). Although cabling is required in this case, one advantage of an Ethernet link is  
9 that radio-frequency interference and jamming are no longer a concern, while another  
10 advantage is that the door access module 604 can actually be powered from the  
11 Ethernet link. Still other options for the communication link 608 will be apparent to  
12 those skilled in the art.

13  
14 The processor 616 runs a registration process 624A and a monitoring process 624B,  
15 both of which will be described in greater detail later on; for now, suffice it to say that  
16 during the registration process 624A for the user 622, the processor 616 looks up the  
17 code 618 and the related access control information 619 for the user 622 in the  
18 memory 612 and sends this data to the door access module 604 to enable access  
19 control to be effected at the door 602 itself. On the other hand, during the monitoring  
20 process 624B, the processor 616 receives information about attempts to open the door  
21 602, logs this information in the memory 612 and may perform further processing.  
22 Some of the further processing may result in an alarm that may be displayed on the  
23 display 626 or conveyed via another output device, such as an antenna in  
24 communication with a wireless device (e.g., SMS-enabled phone, networked wireless  
25 personal digital assistant, etc.)

26  
27 The functionality of the processor 616 may be implemented as pre-programmed  
28 hardware or firmware elements (e.g., application specific integrated circuits (ASICs),  
29 electrically erasable programmable read-only memories (EEPROMs), etc.), or other  
30 related components. In other embodiments, the processor 616 may be implemented as  
31 an arithmetic and logic unit (ALU) or a neural processor having access to a code  
32 memory (not shown) which stores program instructions for the operation of the ALU.  
33 The program instructions could be stored on a medium which is fixed, tangible and  
34 readable directly by the processor 616, (e.g., removable diskette, CD-ROM, ROM,

1 fixed disk, USB drive), or the program instructions could be stored remotely but  
2 transmittable to the processor 616 via a modem or other interface device.

3  
4 With additional reference to Fig. 6B, the door access module 604 includes a biometric  
5 apparatus 630, a controller 632, a communication interface 634 and a memory 644.

6  
7 The biometric apparatus 630, which can be embodied as the biometric apparatus 610,  
8 produces a code 636 on the basis of an object submitted to it by a given user 638 who  
9 is attempting to open the door 602. When the given user 638 is one of the registered  
10 users (e.g., user 622 or other registered user), then it is expected that the object  
11 submitted to the biometric apparatus 630 will be whichever skin-covered body part of  
12 the given user 638 was employed when registering with the management entity 606.  
13 However, it is possible that other objects may be submitted to the biometric apparatus  
14 630 by the given user 638. It is also possible that the given user 638 is not a  
15 registered user.

16  
17 The communication interface 634 is operative to communicate with the management  
18 entity 606. It is also within the scope of the present invention for the communication  
19 interface 634 to allow communication between the door access module 604 and other  
20 door access modules on other doors, or other entities such as communication devices  
21 worn by security guards.

22  
23 The memory 644 stores the codes 618, 618A, 618B and the related access control  
24 information 619, 619A, 619B, as received from the management entity 606 via the  
25 communication interface 634 following registration of various users including user  
26 622.

27  
28 The controller 632 has access to the memory 644, the communication interface 634  
29 and the biometric apparatus 630. The controller 632 runs a registration process 646A  
30 and a monitoring process 646B, both of which will be described in greater detail later  
31 on; for now, suffice it to say that during the registration process 646A, the controller  
32 632 receives codes and related access control information from the management entity  
33 606 via the communication interface 634 and stores this information in the memory  
34 644.

1  
2 During the monitoring process 646B, the controller 632 responds to attempts to open  
3 the door 602 by controlling a door restraint mechanism 648 by wired or wireless  
4 techniques via the communication interface 634. This gives the door access module  
5 604 the ability to release the door 602, thus allowing it to be opened from a closed  
6 state. Any suitable door restraint mechanism 648 can be used, such as latch-based,  
7 electromagnetic, etc. In addition, during the monitoring process 646B, the controller  
8 632 collects information regarding attempts being made to open the door 602 and  
9 sends this information to the management entity 606 via the communication interface  
10 634 (or may keep this information in the memory 644 until receipt of a request from  
11 the management entity 606 to read the information).

12  
13 It is noted that the use of wireless communication between the controller 632 and the  
14 door restraint mechanism 648 may be particularly useful when the door 602 is made  
15 of a material or structure that is not amenable to installation of the door access module  
16 604.

17  
18 In some embodiments (where the door 602 is made of a metal or comprises portions  
19 made of a metal), it may be advantageous to locate the door restraint mechanism 648,  
20 if electromagnetic nature in nature, on or in the door frame. On the other hand, in  
21 some embodiments (where the door restraint mechanism 648 is connected to the door  
22 handle), the door restraint mechanism 648 may be located entirely within or on the  
23 door. Generally, it should be understood that the door restraint mechanism 648 may  
24 have components that reside off of the door 602 and/or components that reside on the  
25 door 602 itself.

26  
27 The functionality of the controller 632 may be implemented as pre-programmed  
28 hardware or firmware elements (e.g., application specific integrated circuits (ASICs),  
29 electrically erasable programmable read-only memories (EEPROMs), etc.), or other  
30 related components. In other embodiments, the controller 632 may be implemented  
31 as an arithmetic and logic unit (ALU) or a neural processor having access to a code  
32 memory (not shown) which stores program instructions for the operation of the ALU.  
33 The program instructions could be stored on a medium which is fixed, tangible and  
34 readable directly by the controller 632, (e.g., removable diskette, CD-ROM, ROM,

1 fixed disk, USB drive), or the program instructions could be stored remotely but  
2 transmittable to the controller 632 via a modem or other interface device.

3  
4 The registration process 624A run by the processor 616 in the management entity 606  
5 and the registration process 646A run by the controller 632 in the door access module  
6 604 are now described with reference to the flow diagram in Fig. 7, for the purposes  
7 of which it is assumed the user 622 is desirous of being registered.

8  
9 Specifically, at step 700 of the registration process 624A, the processor 616 obtains  
10 the access control information 619 regarding the user 622. The access control  
11 information 619 may include, *inter alia*, an identity of the user 622 (e.g., a user ID  
12 660), access restrictions 662 (e.g., time-of day and/or day-of-week), a history of  
13 previous accesses to the door 602, and so on. It should be understood that some of the  
14 access control information 619 may be provided by an external database (not shown).  
15 The access control information 619 for the user 622 is stored in the memory 612.

16  
17 At step 702 of the registration process 624A, the processor 616 obtains the code 618  
18 that the biometric apparatus 610 derives from the user's skin-covered body part 620.  
19 The code 618 is also stored in the memory 612, in association with the access control  
20 information 619 for the user 622.

21  
22 At step 704 of the registration process 624A, and assuming that the user 622 is indeed  
23 authorized to at least sometimes open the door 602, the processor 616 sends the code  
24 618 and the user ID 660 of the user 622 to the door access module 604 via the  
25 communication link 608. If the access control information 619 for the user 622  
26 specifies certain restrictions on the user's access to the door 602, then such access  
27 restrictions 662 are also sent to the door access module 604 via the communication  
28 link 608.

29  
30 At step 706 of the registration process 646A, the controller 632 receives via the  
31 communication interface 634 the code 618, the user ID 660 of the user 622 and  
32 possibly certain access restrictions 662 associated with the user 622. The code 618,  
33 the user ID 660 and the access restrictions 662 (if any) are stored in the memory 644.

1 Of course, the above steps are performed for the various other doors to which the user  
2 622 may have access, as well as for the various other users who undergo registration.  
3 As new users are registered or access restrictions fluctuate, the above steps can be  
4 performed as needed.

5  
6 Also, in an alternative embodiment, step 704 may be performed using an intermediary  
7 such as a smart card. Specifically, the code 618, the user ID 660 of the user 622 and  
8 the relevant access restrictions 662 associated with the user 622 can be placed onto a  
9 medium such as a smart card that is physically transported to the door access module  
10 604, which downloads the information as required.

11  
12 The monitoring process 624B run by the processor 616 in the management entity 606  
13 and the monitoring process 646B run by the controller 632 in the door access module  
14 604 are now described with reference to the flow diagram in Fig. 8, in which an as yet  
15 unidentified person makes an attempt to open the door 602.

16  
17 Specifically, at step 802 of the monitoring process 646B, the controller 632  
18 communicates with the biometric apparatus 630 to obtain a code 650 therefrom. At  
19 this stage, it is still not known whether the person is authorized to open the door 602.

20  
21 At step 804 of the monitoring process 646B, the controller 632 consults the memory  
22 644 and compares the received code 650 to the various codes stored therein (e.g.,  
23 codes 618, 618A, 618B). If there is a match between the code 650 and the code  
24 corresponding to a given registered user, then the next step is step 806; otherwise the  
25 next step is step 812.

26  
27 At step 806 of the monitoring process 646B, the controller 632 extracts from the  
28 memory 644 the user ID (denoted 670) and the access restrictions (denoted 672)  
29 stored in association with the code that matches the code 650 received from the  
30 biometric apparatus 630.

31  
32 At step 808 of the monitoring process 646B, the controller 632 checks the access  
33 restrictions 672 to see whether the person attempting to access has the requisite  
34 authority. Thus, the controller 632 may establish that the person, although registered,



1 does not necessarily have authority to open the door 602 at the current time, or during  
2 the current day of the week, etc. If access is permitted, the next step is step 810;  
3 otherwise the next step is step 812.

4  
5 At step 810 of the monitoring process 646B, the controller 632 sends a signal to the  
6 door restraint mechanism 648, which releases the door 602 and allows it to be opened.  
7 The door restraint mechanism 648 may be configured such that if the door 602 is not  
8 opened after a certain amount of time, the door will once again be restrained. Also,  
9 the door restraint mechanism 648 may be configured such that once the door 602 is  
10 opened, it will once again be restrained as soon as it is closed.

11  
12 At step 812 of the monitoring process 646B, which is optional, the controller 632  
13 reports the result of the current access attempt to the management entity 606 via the  
14 communication interface 634. For example the result of the current access attempt  
15 may be “success for user ID xyz”, “failure due to unrecognized user”, “failure for user  
16 ID xyz due to unauthorized time period”, etc. Here, “xyz” refers to the information  
17 conveyed by the user ID 672.

18  
19 It is noted that if step 812 is reached directly from step 804 or step 808, then step 810  
20 will not be performed and hence the door 602 will remain closed under the effect of  
21 the door restraint mechanism 648.

22  
23 At step 814 of the monitoring process 624B, the processor 616 receives the result of  
24 the current access attempt via the communication interface 614. If the result is  
25 “success for user ID xyz” or “failure for user ID xyz due to unauthorized time period”,  
26 the result may simply be stored in the memory 612 as part of the access control  
27 information (specifically, the history of previous accesses to) for the user having user  
28 ID xyz.

29  
30 At step 816 of the monitoring process 624B, the processor 616 verifies certain  
31 conditions and if they are met, signals an alarm. This can be done when the result of  
32 the current access attempt is “failure due to unrecognized user”, which may cause the  
33 processor 616 to trigger an alarm to be displayed over the display 626 or conveyed  
34 over another output device, or relayed to a security guard, etc. An alarm could also be

1 triggered under a variety of other conditions, even if the person attempting to open the  
2 door 602 is a registered user. For example, if the same registered user goes in and out  
3 too often, or if a registered user makes multiple failed attempts during a restricted  
4 time period, or if a registered user appears to be going through two different doors at  
5 about the same time, etc.

6  
7 In a variant of the above-described embodiment, one may eliminate steps 704 and 706  
8 of the registration process, while making steps 804 to 806 the responsibility of the  
9 processor 606 in the management entity 616. The scenario envisaged by this variant  
10 is one in which there is minimal processing done at the door access module 604, with  
11 the exception of code generation. Specifically, the code derived from a skin-covered  
12 body part would be sent to the controller 616 in the management entity 606. The  
13 controller 616 would then be responsible for verifying whether there is a match with  
14 any of the codes that correspond to people authorized to enter through the door 602 at  
15 the given time. If a match is found, the controller 616 would send a signal to the  
16 controller 632 which, in turn, causes the controller 632 to send a signal to the door  
17 restraint mechanism 648 to allow the door 602 to be opened. It is therefore seen that  
18 most of the comparison is centralized at the management entity 606, which may  
19 simplify access management and may allow the implementation of less expensive  
20 door access modules 604.

21  
22 In view of the foregoing, it is noted that use of biometrics, and more specifically skin-  
23 covered body parts, in the above system allows authentication of registered users to be  
24 achieved to a high degree of accuracy. Meanwhile, the information stored in the  
25 memory 612 of the management entity 606 (and in the memory 644 of the door access  
26 module 604) is of a nature that does not allow a malicious user who obtains this  
27 information to extract any meaningful personal information about the registered users.  
28 In addition, the use of a controller local to each door reduces the power consumption  
29 of the door access module 604, to a point where connection to the standard AC power  
30 grid is not required. This, in turn, has the effect of reducing the installation cost for  
31 the door access module 604. Of course, the option still exists to connect the door  
32 access module 604 to the AC power grid.

1    Application #2: Offender Supervision

2  
3    “House arrest” allows an offender who is sentenced to a jail term to spend the time at  
4    his or her home as an alternative to being physically confined to jail. In some cases, it  
5    is necessary to confirm that the offender is indeed at home. With reference now to  
6    Fig. 9, there is shown a system for electronic supervision of offenders under  
7    conditions of house arrest, in accordance with an embodiment of the present  
8    invention. The system includes a management entity 902 and a remote unit 904. It is  
9    envisaged that the management entity 902 may be located, for example, at a  
10   corrections center or government office, whereas the remote unit 904 is located at a  
11   residential address or other location where an offender 906 is required to be physically  
12   located at certain specified times.

13  
14   Communication between the management entity 902 and the remote unit 904 is  
15   established over one or more networks 918. A suitable example of a network 918  
16   between the management entity 902 and the remote unit 904 is the PSTN. In such a  
17   case, it is envisaged that the remote unit 904 may be connected to a conventional  
18   telephone outlet at the aforementioned residential address. Still other arrangements  
19   are possible, such as connection via a cable distribution network, fixed wireless  
20   network, data network, etc.

21  
22   The management entity 902 includes a memory 908 that stores a code (or a plurality  
23   of codes) 910 representative of a skin-covered body part 912 of the offender 906. It is  
24   assumed that the code (or codes) 910 will have been derived from the offender’s skin-  
25   covered body part 912 during a registration process, using a technique that is based on  
26   geometric measures of combinations of pixels taken from a plurality of subsets of  
27   like-shaded pixels in an image of the skin-covered body part 912. An example of a  
28   suitable technique for generation of the code (or codes) 910 may be based on that  
29   described above with reference to Fig. 3. A plurality of codes 910 may be used to  
30   reduce the rate of false rejection, by accounting for slight deviations in the result of  
31   encoding images acquired from real-life body parts.

32  
33   The management entity 902 also includes a processor 913 and a communication  
34   interface 914. The communication interface 914 connects the management entity 902

1 to the aforementioned one or more networks 918 (e.g., the PSTN). In a specific non-  
2 limiting example embodiment, the communication interface 914 is a modem. The  
3 processor 913 runs a supervision process 920, which will be described in greater  
4 detail later on; for now, suffice it to say that the supervision process 920 operates to  
5 assess whether a code received from the remote unit 904 is representative of the skin-  
6 covered body part 912 of the offender 906. The management entity 902 further  
7 includes a display 930 or other output device, for communicating the result of the  
8 supervision process to an operator or a command station, for example.

9  
10 The functionality of the processor 913 may be implemented as pre-programmed  
11 hardware or firmware elements (e.g., application specific integrated circuits (ASICs),  
12 electrically erasable programmable read-only memories (EEPROMs), etc.), or other  
13 related components. In other embodiments, the processor 913 may be implemented as  
14 an arithmetic and logic unit (ALU) or a neural processor having access to a code  
15 memory (not shown) which stores program instructions for the operation of the ALU.  
16 The program instructions could be stored on a medium which is fixed, tangible and  
17 readable directly by the processor 913, (e.g., removable diskette, CD-ROM, ROM,  
18 fixed disk, USB drive), or the program instructions could be stored remotely but  
19 transmittable to the processor 913 via a modem or other interface device.

20  
21 The remote unit 904 includes a biometric apparatus 922, a communication interface  
22 924 and a controller 926. The biometric apparatus 922 produces a code 928 on the  
23 basis of an object submitted to it. In the expected scenario, the object submitted to the  
24 biometric apparatus 922 is the skin-covered body part 912 of the offender 906.  
25 However, it is possible that other objects may be submitted to the biometric apparatus  
26 922, which may especially occur when the offender 906 is attempting to “fool” the  
27 management entity 902 into believing that he or she is present, or quite simply, when  
28 the offender 906 is absent.

29  
30 In order to reduce the likelihood of transmitting personal information over the one or  
31 more networks 918, the code 928 output by the biometric apparatus 922 should not  
32 provide information allowing reconstruction of a meaningful image of the skin-  
33 covered body part 912. To this end, the biometric apparatus 922 is preferably the  
34 biometric apparatus 12 described above with references to Figs. 1-4, 5A and 5B.



1  
2 The communication interface 924 connects the remote unit 904 to the aforementioned  
3 one or more networks 918 (e.g., the PSTN). In a specific non-limiting example  
4 embodiment, the communication interface 924 is a modem. The controller 926 runs a  
5 gathering process 932 that communicates with the management entity 902 via the  
6 communication interface 924, and also with the biometric apparatus 922.

7  
8 The functionality of the controller 926 may be implemented as pre-programmed  
9 hardware or firmware elements (e.g., application specific integrated circuits (ASICs),  
10 electrically erasable programmable read-only memories (EEPROMs), etc.), or other  
11 related components. In other embodiments, the controller 926 may be implemented  
12 as an arithmetic and logic unit (ALU) or a neural processor having access to a code  
13 memory (not shown) which stores program instructions for the operation of the ALU.  
14 The program instructions could be stored on a medium which is fixed, tangible and  
15 readable directly by the controller 926, (e.g., removable diskette, CD-ROM, ROM,  
16 fixed disk, USB drive), or the program instructions could be stored remotely but  
17 transmittable to the controller 926 via a modem or other interface device.

18  
19 The gathering process 932, in conjunction with the supervision process 920 run by the  
20 processor 913 of the management entity 902, will now be described in greater detail  
21 with reference to Fig. 10.

22  
23 Specifically, at step 1002, the processor 913 in the management entity 902 begins by  
24 determining that it is time to gather presence information regarding the offender 906.  
25 This determination may be made on a basis of a pre-determined schedule or it can be  
26 made on a basis of having received an operator request. The processor 913 contacts  
27 the remote unit 904 using the communication interface 914, which causes the  
28 gathering process 932 to be invoked at the remote unit 904. Accordingly, the  
29 processor 913 in the management entity 902 and the controller 926 in the remote unit  
30 904 establish communication with one another (e.g., by a handshaking protocol  
31 involving the communication interfaces 914 and 924, respectively).

32  
33 At step 1006, the controller 926 in the remote unit 904 prompts the offender 906 to  
34 submit the skin-covered body part 912. This can be done via an output device (not



1 shown), such as by emitting a tone or message over a loudspeaker. After a certain  
2 grace period (e.g., 30 seconds), the controller 926 communicates with the biometric  
3 apparatus 922 at step 1008 to obtain a code 928 therefrom. Of course, the controller  
4 926 does not know whether the offender 906 has actually placed his or her body part  
5 912 onto the platen of the biometric apparatus 922. In fact, it may not even be known  
6 whether anything at all was submitted to the biometric apparatus 922. Thus, the code  
7 928 provided by the biometric apparatus 922 will be derived from an image of an  
8 apparent object that may or may not be the skin-covered body part 912.

9  
10 In order to make an assessment of whether or not the skin-covered body part 912 was  
11 submitted to the biometric apparatus 922, step 1010 consists of the controller 926  
12 releasing the code 928 to the management entity 902 via the communication interface  
13 924 and the one or more networks 918. This signals the end of the gathering process  
14 932. Meanwhile, the code 928 is received at the communication interface 914 of the  
15 management entity 902 and is processed by the processor 913.

16  
17 Specifically, at step 1012, the processor 913 consults the memory 908 and compares  
18 the code 928 to the code (or codes) 910, which are known to have been derived from  
19 an acquired image of the offender's skin-covered body part 912. If the comparison  
20 yields a match between the code 928 and the code 910 (or any of the codes 910 when  
21 there are more than one) in the memory 908, then presence of the offender 906 is  
22 deemed verified and the result of the supervision process 920 is considered to be a  
23 success; otherwise presence of the offender 906 is deemed not verified and the result  
24 of the supervision process 920 is considered to be a failure. At step 1014, the  
25 processor 913 may signal the result of the supervision process 920 via the display 930  
26 or other output device.

27  
28 Of course, variations of the above are possible. For example, at step 1012, even if the  
29 comparison does not yield a match between the code 928 and the code 910 (or any of  
30 the codes 910 when there are more than one), then it is within the scope of the present  
31 invention to allow a limited number of "re-tries" to further reduce the false rejection  
32 rate. Specifically, the biometric apparatus 922 derives additional codes from acquired  
33 images of whatever is deemed to have been submitted to it. In this way, a poorly

1 positioned body part may be repositioned with a greater chance of the supervision  
2 process 920 yielding a successful result.

3  
4 Also, it is envisaged that the determination as when to gather presence information  
5 regarding the offender 906 may be programmed within the controller 926 of the  
6 remote unit 904 (rather than the management entity 902). Hence, step 1004, by virtue  
7 of which communication between the management entity 902 and the remote unit 904  
8 is established, would be initiated by the controller 926 in the remote unit 904.

9  
10 Additionally, it should be understood that for added security, the code 928 may itself  
11 include encrypted information, or the code 928 may be encrypted by the controller  
12 926 in the remote unit 904 and decrypted by the processor 913 in the management  
13 entity 902.

14  
15 In view of the foregoing, it is noted that use of biometrics, and more specifically skin-  
16 covered body parts, in the above system allows the presence of the offender 906 to be  
17 verified to a high degree of accuracy. Meanwhile, the information exchanged  
18 between the management entity 902 and the remote unit 904 (and stored in the  
19 memory 908) is of a nature that does not allow a malicious user who intercepts this  
20 information, and possibly even decrypts it, to obtain any meaningful personal  
21 information about the offender 906. In addition, the amount of information  
22 exchanged over the one or more networks 18 is sufficiently small that it can be  
23 transmitted to the management entity 902 in a reasonable amount of time.

24  
25 It will be appreciated that the system described above may be used in an identical  
26 fashion to enable parents to electronically supervise their children or in any other  
27 situation where it is desired to “check up” on individuals expected to be at a fixed  
28 location.

29  
30 Those skilled in the art will be able to conceive of still further applications of the  
31 biometric apparatus 12 and the techniques used by the biometric apparatus 12 to  
32 derive a code from an acquired image of a skin-covered body part.

1 While specific embodiments of the present invention have been described and  
2 illustrated, it will be apparent to those skilled in the art that numerous modifications  
3 and variations can be made without departing from the scope of the invention as  
4 defined in the appended claims.

5